Instituto Tecnológico de Cancún

Materia:

Fundamentos de Telecomunicaciones

Tarea:

Laboratorio 5

Set Key WireShark Preferences(IMPORTANT LAB)

Alumno: **Aguilar Moreno Jorge Axel**

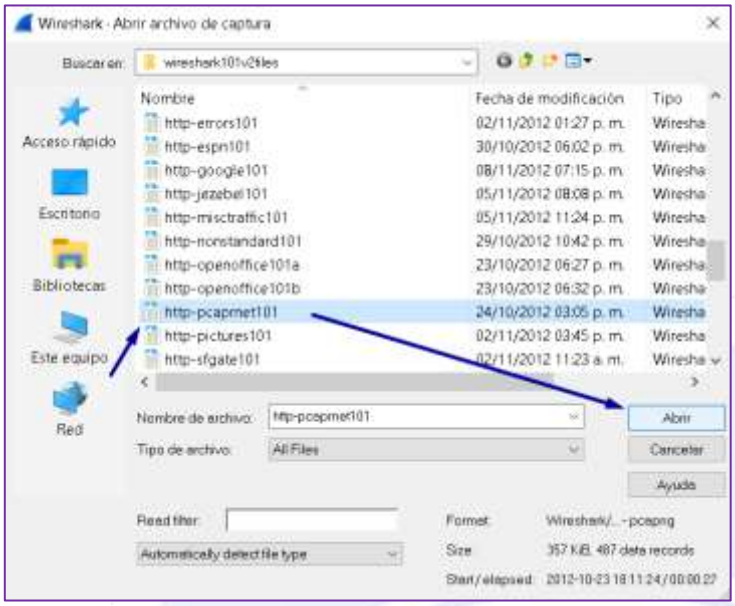
Docente: **Ismael Jiménez Sánchez**

Horario: **17:00 – 18:00**

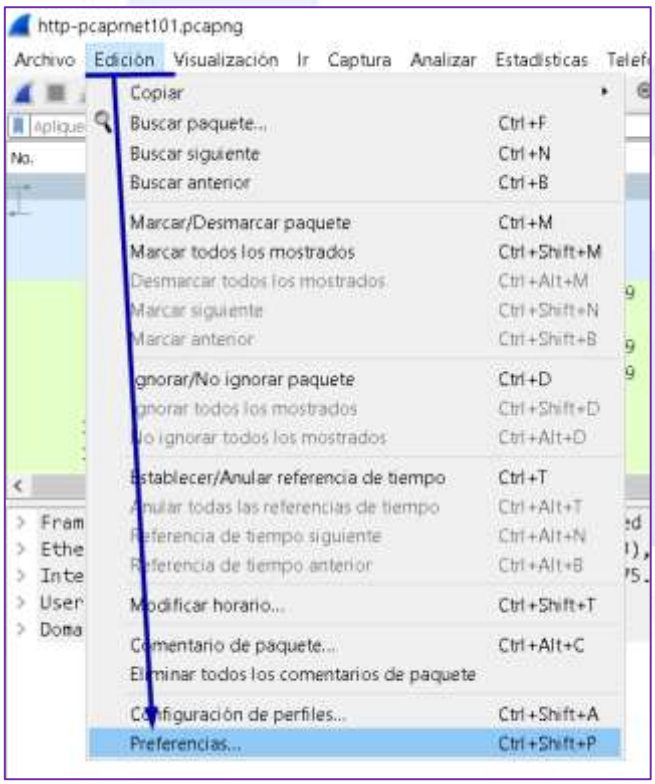
Ing. **Sistemas Computacionales**

5.-Semestre

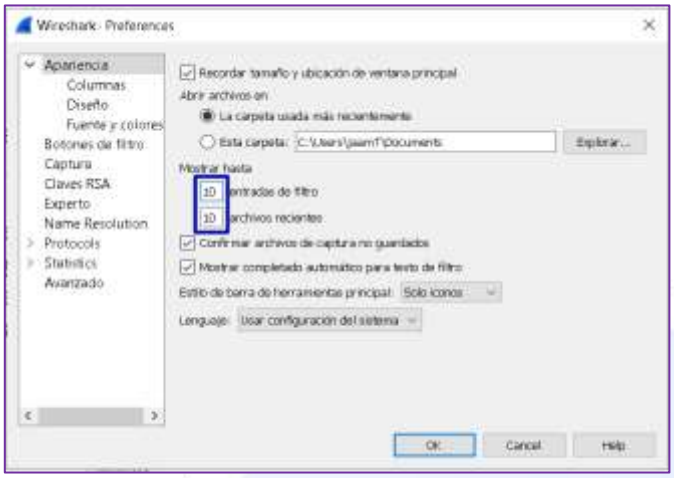
Paso 1:

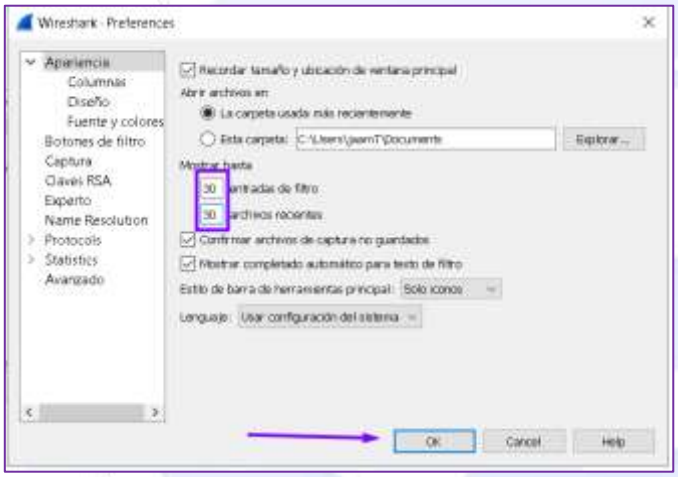

Wireshark · Abrir archivo de captura
Buscar en:
wireshark101v2files
Acceso rápido
Escritorio
Bibliotecas
Este equipo
Red
Nombre
Fecha de modificación
Tipo
http-errors101
http-espn101
http-google101
http-jezebel101
http-misctraffic101
http-nonstandard101
http-openoffice101a
http-openoffice101b
http-pcapnet101
http-pictures101
http-sfgate101
Nombre de archivo:
http-pcapnet101
Tipo de archivo:
All Files
Abrir
Cancelar
Ayuda
Read filter:
Automatically detect file type
Format:
Size
Start / elapsed:

Paso 2:

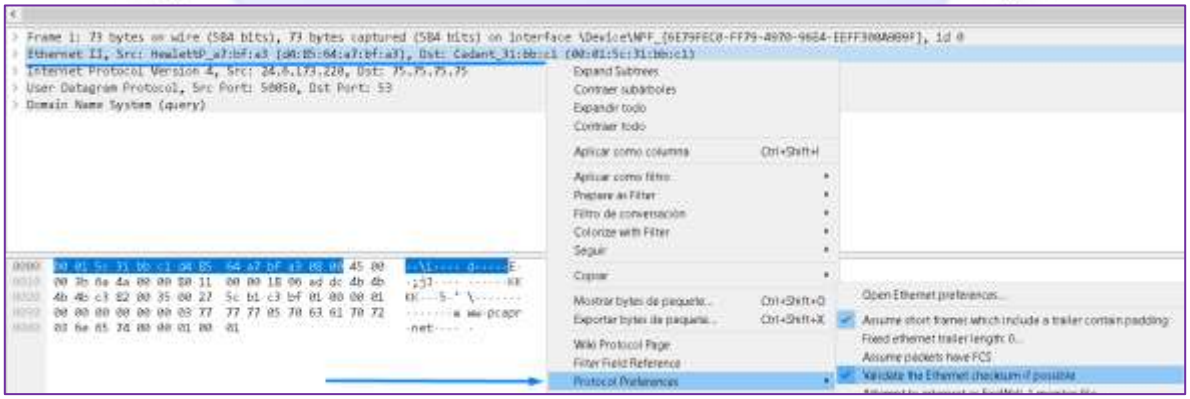

http-pcapnet101.pcapng
Archivo
Edición
Visualización
Ir
Captura
Analizar
Estadísticas
Copiar
Buscar paquete... Ctrl+F
Buscar siguiente Ctrl+N
Buscar anterior Ctrl+B
Marcar/Desmarcar paquete Ctrl+M
Marcar todos los mostrados Ctrl+Shift+M
Desmarcar todos los mostrados Ctrl+Alt+M
Marcar siguiente Ctrl+Shift+N
Marcar anterior Ctrl+Shift+B
Establecer/Anular referencia de tiempo Ctrl+T
Modificar horario... Ctrl+Shift+T
Comentario de paquete... Ctrl+Alt+C
Eliminar todos los comentarios de paquete
Preferencias... Ctrl+Shift+P

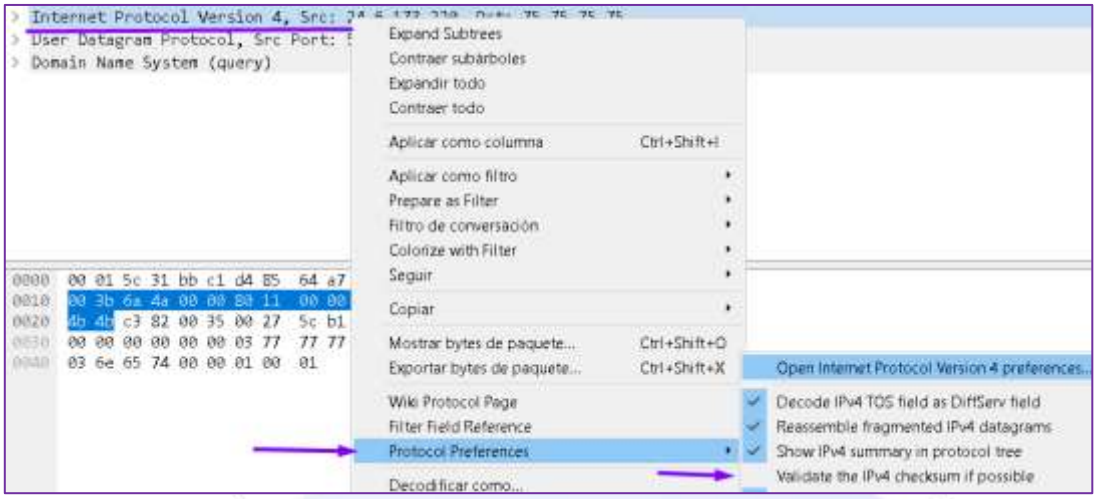
Paso 3:

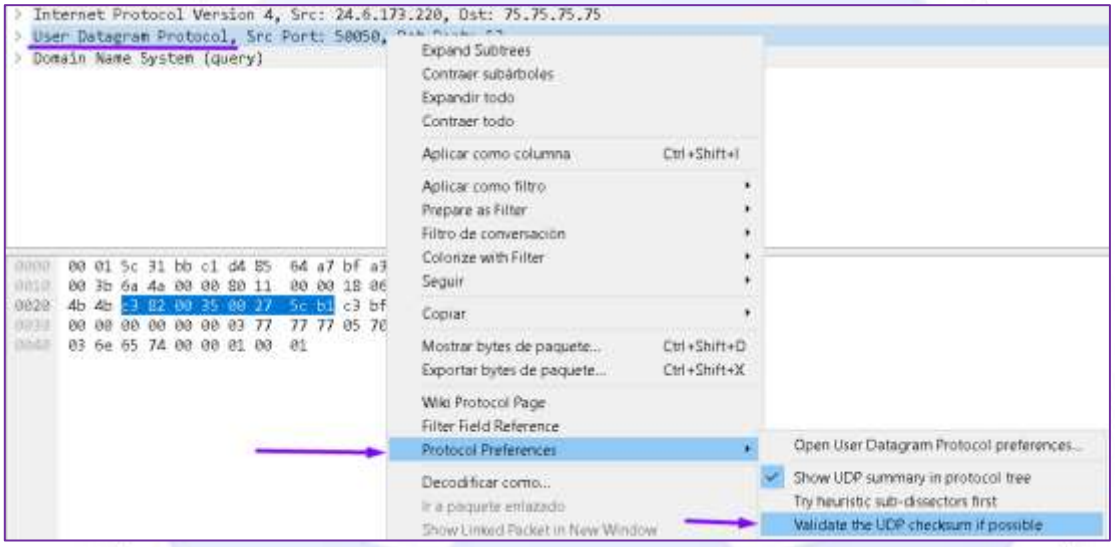

Wireshark · Preferences
Apariencia
Columnas
Diseño
Fuente y colores
Botones de filtro
Captura
Claves RSA
Experto
Name Resolution
Protocols
Statistics
Avanzado
Recordar tamaño y ubicación de ventana principal
Abrir archivos en:
La carpeta usada más recientemente
Esta carpeta:
C:\Users\jaamT\Documents
Explorar...
Mostrar hasta
10
entradas de filtro
10
archivos recientes
Confirmar archivos de captura no guardados
Mostrar completado automático para texto de filtro
Estilo de barra de herramientas principal:
Solo iconos
Lenguaje:
Usar configuración del sistema
OK
Cancel
Help

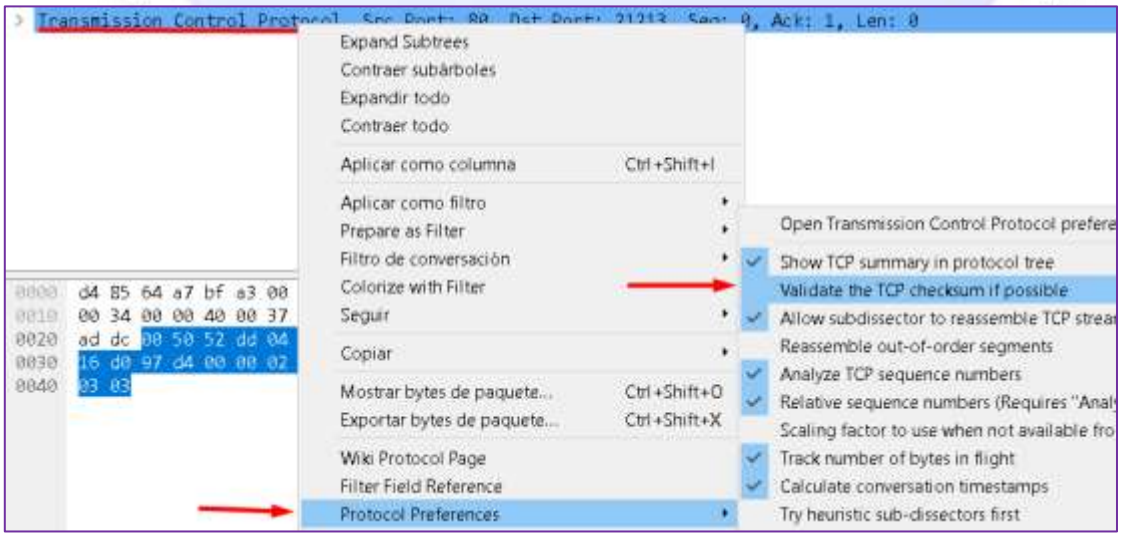

Wireshark · Preferences
Apariencia
Columnas
Diseño
Fuente y colores
Botones de filtro
Captura
Claves RSA
Experto
Name Resolution
Protocols
Statistics
Avanzado
Recordar tamaño y ubicación de ventana principal
Abrir archivos en:
La carpeta usada más recientemente
Esta carpeta:
C:\Users\jaamT\Documents
Explorar...
Mostrar hasta
30
entradas de filtro
30
archivos recientes
Confirmar archivos de captura no guardados
Mostrar completado automático para texto de filtro
Estilo de barra de herramientas principal:
Solo iconos
Lenguaje:
Usar configuración del sistema
OK
Cancel
Help

Paso 4:

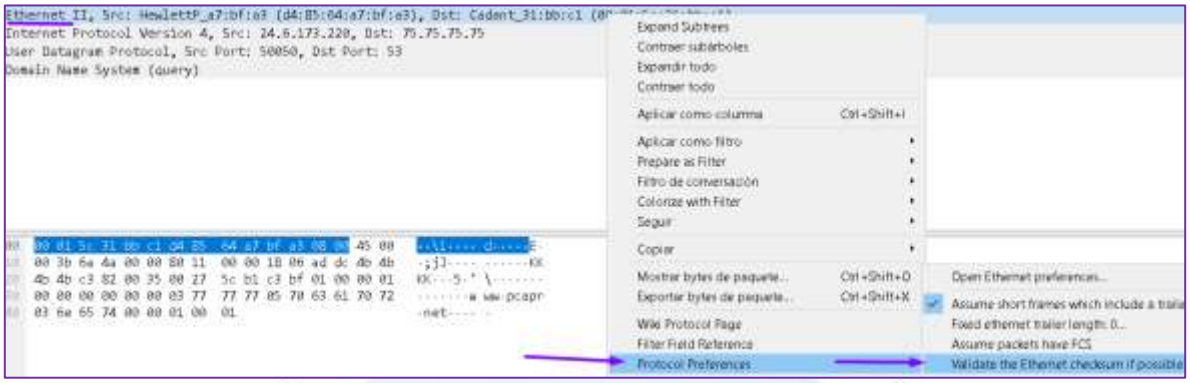

Frame 1: 73 bytes on wire (584 bits), 73 bytes captured (584 bits) on interface \Device\NPF_{6E79FEC0-FF79-4970-9684-EEFF300A889F}, id 0
Ethernet II, Src: HewlettP_a7:bf:a3 (d4:85:64:a7:bf:a3), Dst: Cadant_31:bb:c1 (00:01:5c:31:bb:c1)
Internet Protocol Version 4, Src: 24.6.173.220, Dst: 75.75.75.75
User Datagram Protocol, Src Port: 50050, Dst Port: 53
Domain Name System (query)
Expand Subtrees
Contraer subárboles
Expandir todo
Contraer todo
Aplicar como columna
Ctrl+Shift+I
Aplicar como filtro
Preparar un Filtro
Filtro de conversación
Colorize with Filter
Seguir
Copiar
Mostrar bytes de paquete...
Ctrl+Shift+O
Exportar bytes de paquete...
Ctrl+Shift+X
Wiki Protocol Page
Filter Field Reference
Protocol Preferences
Open Ethernet preferences...
Assume short frames which include a trailer contain padding
Fixed ethernet trailer length: 0...
Assume packets have FCS
Validate the Ethernet checksum if possible


Internet Protocol Version 4, Src:
User Datagram Protocol, Src Port:
Domain Name System (query)
Expand Subtrees
Contraer subárboles
Expandir todo
Contraer todo
Aplicar como columna Ctrl+Shift+I
Aplicar como filtro
Prepare as Filter
Filtro de conversación
Colorize with Filter
Seguir
Copiar
Mostrar bytes de paquete... Ctrl+Shift+O
Exportar bytes de paquete... Ctrl+Shift+X
Wiki Protocol Page
Filter Field Reference
Protocol Preferences
Decodificar como...
Open Internet Protocol Version 4 preferences...
Decode IPv4 TOS field as DiffServ field
Reassemble fragmented IPv4 datagrams
Show IPv4 summary in protocol tree
Validate the IPv4 checksum if possible

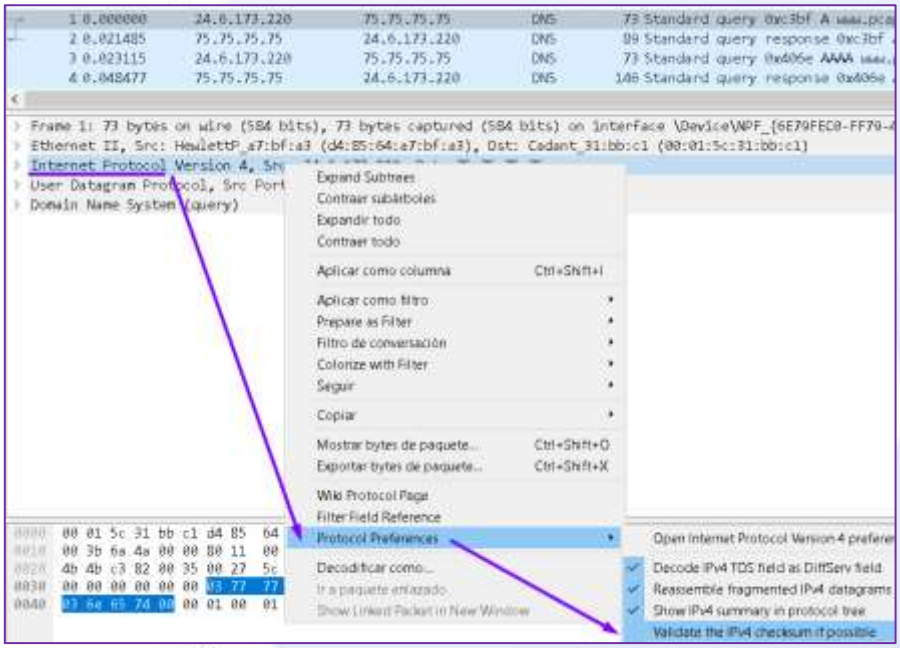

Internet Protocol Version 4, Src: 24.6.173.220, Dst: 75.75.75.75
User Datagram Protocol, Src Port: 50050,
Domain Name System (query)
Expand Subtrees
Contraer subárboles
Expandir todo
Contraer todo
Aplicar como columna Ctrl+Shift+I
Aplicar como filtro
Prepare as Filter
Filtro de conversación
Colorize with Filter
Seguir
Copiar
Mostrar bytes de paquete... Ctrl+Shift+O
Exportar bytes de paquete... Ctrl+Shift+X
Wiki Protocol Page
Filter Field Reference
Protocol Preferences
Decodificar como...
Ir a paquete enlazado
Show Linked Packet in New Window
Open User Datagram Protocol preferences...
Show UDP summary in protocol tree
Try heuristic sub-dissectors first
Validate the UDP checksum if possible

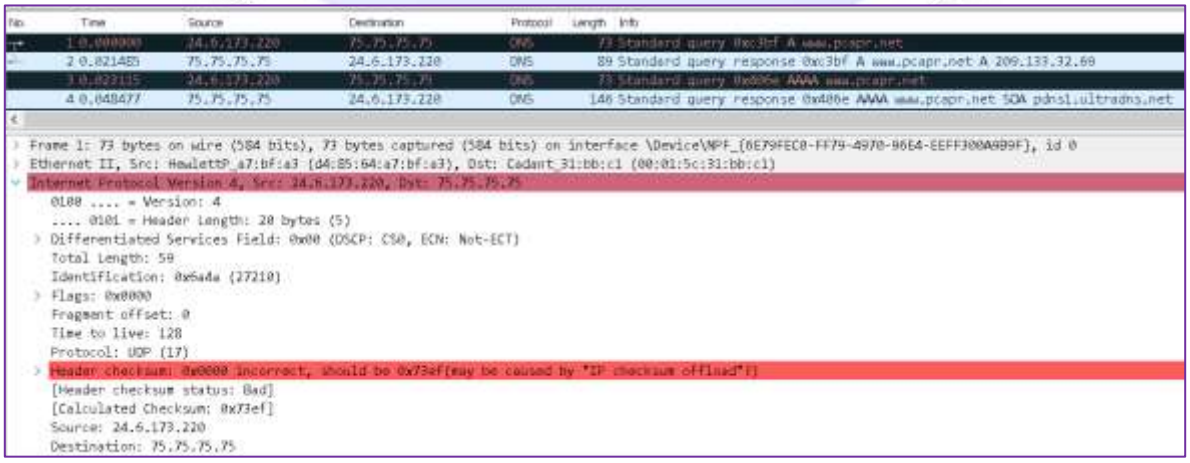

Transmission Control Protocol
Ack: 1, Len: 0
Expand Subtrees
Contraer subárboles
Expandir todo
Contraer todo
Aplicar como columna Ctrl+Shift+I
Aplicar como filtro
Prepare as Filter
Filtro de conversación
Colorize with Filter
Seguir
Copiar
Mostrar bytes de paquete... Ctrl+Shift+O
Exportar bytes de paquete... Ctrl+Shift+X
Wiki Protocol Page
Filter Field Reference
Protocol Preferences
Open Transmission Control Protocol prefere
Show TCP summary in protocol tree
Validate the TCP checksum if possible
Allow subdissector to reassemble TCP strea
Reassemble out-of-order segments
Analyze TCP sequence numbers
Relative sequence numbers (Requires "Anal
Scaling factor to use when not available fro
Track number of bytes in flight
Calculate conversation timestamps
Try heuristic sub-dissectors first

Paso 5:

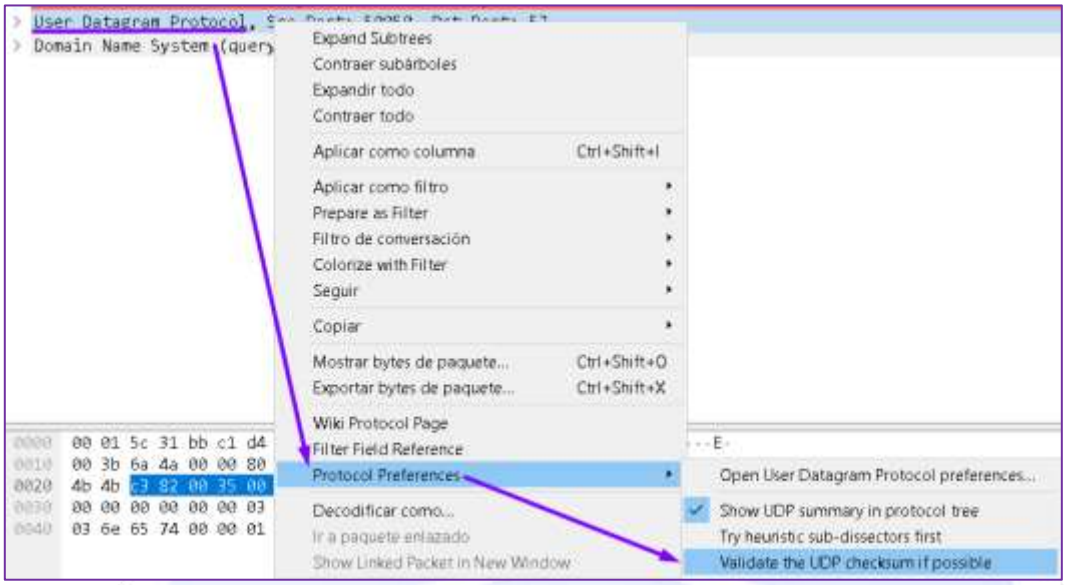

Ethernet II, Src: HewlettP_a7:bf:a3 (d4:85:64:a7:bf:a3), Dst: Cadant_31:bb:c1
Internet Protocol Version 4, Src: 24.6.173.220, Dst: 75.75.75.75
User Datagram Protocol, Src Port: 50050, Dst Port: 53
Domain Name System (query)
Expand Subtrees
Contraer subárboles
Expandir todo
Contraer todo
Aplicar como columna Ctrl+Shift+I
Aplicar como filtro
Prepare as Filter
Filtro de conversación
Colorize with Filter
Seguir
Copiar
Mostrar bytes de paquete... Ctrl+Shift+O
Exportar bytes de paquete... Ctrl+Shift+X
Wiki Protocol Page
Filter Field Reference
Protocol Preferences
Open Ethernet preferences...
Assume packets have FCS
Validate the Ethernet checksum if possible

Paso 6:


1 0.000000 24.6.173.220 75.75.75.75 DNS 73 Standard query 0xc3bf A www.pca
2 0.021485 75.75.75.75 24.6.173.220 DNS 89 Standard query response 0xc3bf
3 0.023115 24.6.173.220 75.75.75.75 DNS 73 Standard query 0x606e AAAA www.
4 0.048477 75.75.75.75 24.6.173.220 DNS 146 Standard query response 0x606e
Frame 1: 73 bytes on wire (584 bits), 73 bytes captured (584 bits) on interface \Device\NPF_{6E79FEC0-FF79-
Ethernet II, Src: HewlettP_a7:bf:a3 (d4:85:64:a7:bf:a3), Dst: Cadant_31:bb:c1 (00:01:5c:31:bb:c1)
Internet Protocol Version 4, Src
User Datagram Protocol, Src Port
Domain Name System (query)
Expand Subtrees
Contraer subárboles
Expandir todo
Contraer todo
Aplicar como columna Ctrl+Shift+I
Aplicar como filtro
Prepare as Filter
Filtro de conversación
Colorize with Filter
Seguir
Copiar
Mostrar bytes de paquete... Ctrl+Shift+O
Exportar bytes de paquete... Ctrl+Shift+X
Wiki Protocol Page
Filter Field Reference
Protocol Preferences
Decodificar como...
Ir a paquete enlazado
Show Linked Packet in New Window
Open Internet Protocol Version 4 prefere
Decode IPv4 TOS field as DiffServ field
Reassemble fragmented IPv4 datagrams
Show IPv4 summary in protocol tree
Validate the IPv4 checksum if possible

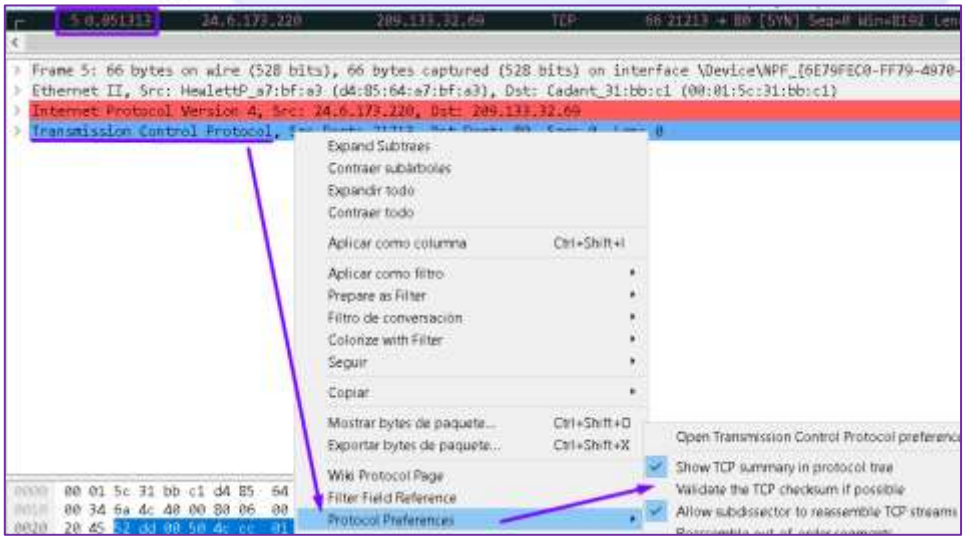

No. Time Source Destination Protocol Length Info
1 0.000000 24.6.173.220 75.75.75.75 DNS 73 Standard query 0xc3bf A www.pcapr.net
2 0.021485 75.75.75.75 24.6.173.220 DNS 89 Standard query response 0xc3bf A www.pcapr.net A 209.133.32.60
3 0.023115 24.6.173.220 75.75.75.75 DNS 73 Standard query 0x606e AAAA www.pcapr.net
4 0.048477 75.75.75.75 24.6.173.220 DNS 146 Standard query response 0x606e AAAA www.pcapr.net SOA pdns1.ultradns.net
Frame 1: 73 bytes on wire (584 bits), 73 bytes captured (584 bits) on interface \Device\NPF_{6E79FEC0-FF79-4970-96E4-EEFF300A999F}, id 0
Ethernet II, Src: HewlettP_a7:bf:a3 (d4:85:64:a7:bf:a3), Dst: Cadant_31:bb:c1 (00:01:5c:31:bb:c1)
Internet Protocol Version 4, Src: 24.6.173.220, Dst: 75.75.75.75
0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 59
Identification: 0x6a4a (27210)
Flags: 0x0000
Fragment offset: 0
Time to live: 128
Protocol: UDP (17)
Header checksum: 0x0000 incorrect, should be 0x73ef(may be caused by "IP checksum offload")
[Header checksum status: Bad]
[Calculated Checksum: 0x73ef]
Source: 24.6.173.220
Destination: 75.75.75.75

Paso 7:


User Datagram Protocol
Domain Name System (query)
Expand Subtrees
Contraer subárboles
Expandir todo
Contraer todo
Aplicar como columna Ctrl+Shift+I
Aplicar como filtro
Prepare as Filter
Filtro de conversación
Colorize with Filter
Seguir
Copiar
Mostrar bytes de paquete... Ctrl+Shift+O
Exportar bytes de paquete... Ctrl+Shift+X
Wiki Protocol Page
Filter Field Reference
Protocol Preferences
Decodificar como...
Ir a paquete enlazado
Show Linked Packet in New Window
Open User Datagram Protocol preferences...
Show UDP summary in protocol tree
Try heuristic sub-dissectors first
Validate the UDP checksum if possible

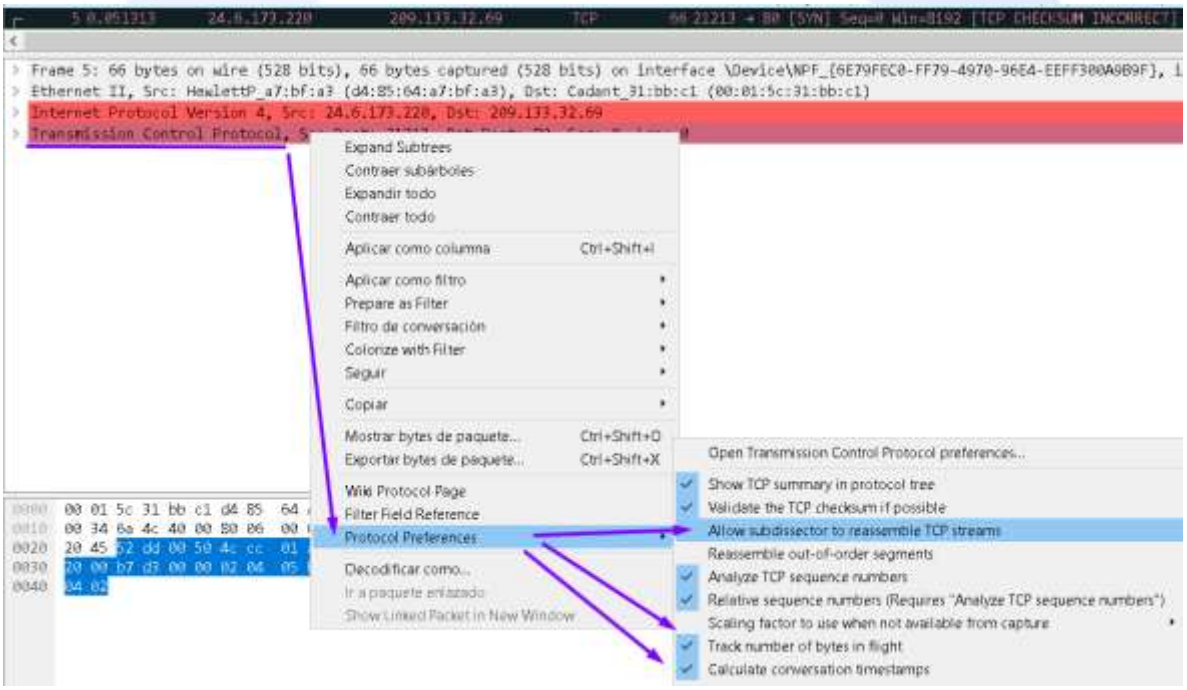

Frame 1: 73 bytes on wire (584 bits), 73 bytes captured (584 bits) on interface \Device\NPF_{6E79FEC0-FF79-4970-96E4-EEFF300A608F}, id 0
Ethernet II, Src: HewlettP_a7:bf:a3 (d4:85:64:a7:bf:a3), Dst: Cadant_31:bb:c1 (00:01:5c:31:bb:c1)
Internet Protocol Version 4, Src: 24.6.173.220, Dst: 75.75.75.75
User Datagram Protocol, Src Port: 50050, Dst Port: 53
Source Port: 50050
Destination Port: 53
Length: 39
[Checksum Status: Bad]
[Stream index: 0]
[Timestamps]
Domain Name System (query)

Paso 8:

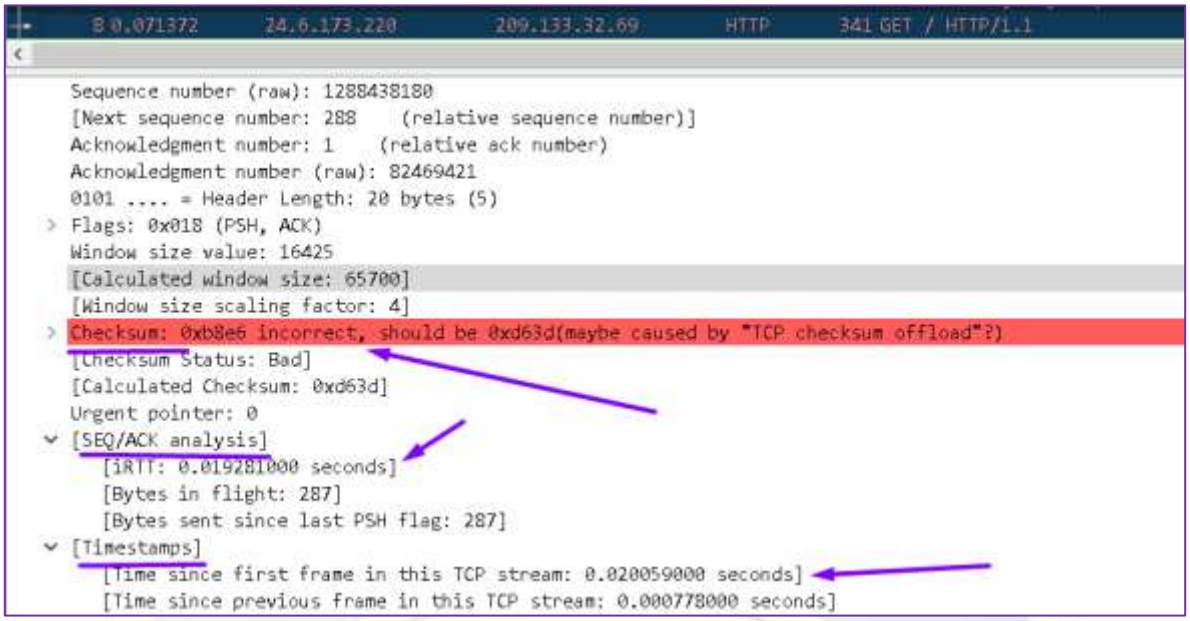

Frame 5: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF_{6E79FEC0-FF79-4970-
Ethernet II, Src: HewlettP_a7:bf:a3 (d4:85:64:a7:bf:a3), Dst: Cadant_31:bb:c1 (00:01:5c:31:bb:c1)
Internet Protocol Version 4, Src: 24.6.173.220, Dst: 209.133.32.69
Transmission Control Protocol,
Expand Subtrees
Contraer subárboles
Expandir todo
Contraer todo
Aplicar como columna Ctrl+Shift+I
Aplicar como filtro
Prepare as Filter
Filtro de conversación
Colorize with Filter
Seguir
Copiar
Mostrar bytes de paquete... Ctrl+Shift+O
Exportar bytes de paquete... Ctrl+Shift+X
Wiki Protocol Page
Filter Field Reference
Protocol Preferences
Open Transmission Control Protocol preferenc
Show TCP summary in protocol tree
Validate the TCP checksum if possible
Allow subdissector to reassemble TCP streams

```
    5 0.051313      24.6.173.220        209.133.32.69       TCP         66 21213 → 80 [
    6 0.070396      209.133.32.69       24.6.173.220        TCP         66 80 → 21213 [
> Frame 5: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\N
> Ethernet II, Src: HewlettP_a7:bf:a3 (d4:85:64:a7:bf:a3), Dst: Cadant_31:bb:c1 (00:01:5c:3
> Internet Protocol Version 4, Src: 24.6.173.220, Dst: 209.133.32.69
v Transmission Control Protocol, Src Port: 21213, Dst Port: 80, Seq: 0, Len: 0
    Source Port: 21213
    Destination Port: 80
    [Stream index: 0]
    [TCP Segment Len: 0]
    Sequence number: 0    (relative sequence number)
    Sequence number (raw): 1288438179
    [Next sequence number: 1    (relative sequence number)]
    Acknowledgment number: 0
    Acknowledgment number (raw): 0
    1000 .... = Header Length: 32 bytes (8)
  > Flags: 0x002 (SYN)
    Window size value: 8192
    [Calculated window size: 8192]
  > Checksum: 0xb7d3 incorrect, should be 0xf5cc(maybe caused by "TCP checksum offload"?)
```

Paso 9:



Paso 10:


8 0.071372 24.6.173.220 209.133.32.69 HTTP 341 GET / HTTP/1.1
Sequence number (raw): 1288438180
[Next sequence number: 288 (relative sequence number)]
Acknowledgment number: 1 (relative ack number)
Acknowledgment number (raw): 82469421
0101 .... = Header Length: 20 bytes (5)
Flags: 0x018 (PSH, ACK)
Window size value: 16425
[Calculated window size: 65700]
[Window size scaling factor: 4]
Checksum: 0xb8e6 incorrect, should be 0xd63d(maybe caused by "TCP checksum offload"?)
[Checksum Status: Bad]
[Calculated Checksum: 0xd63d]
Urgent pointer: 0
[SEQ/ACK analysis]
[iRTT: 0.019281000 seconds]
[Bytes in flight: 287]
[Bytes sent since last PSH flag: 287]
[Timestamps]
[Time since first frame in this TCP stream: 0.020059000 seconds]
[Time since previous frame in this TCP stream: 0.000778000 seconds]